# Appendix E

# Oracle Security CHECKLIST

**Topic:** **Database Management System**
**SubTopic:** **File System Security**

***Objective 205***
Verify that application files are stored on the recommended drives/devices.

***Rationale:***
To protect the system database since it contains all system data and to protect the audit database.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Store the control and data files, the redo log files, and the audit files on separate drives.

***Expected Results:***

***Comments:***
In case of a failure, the data can be retrieved from the redo logs which are stored on a separate disk.

**Topic:** **Database Management System**
**SubTopic:** **File System Security**

***Objective 207***
Verify the application directory is owned by the proper user and the file permissions are set correctly.

***Rationale:***
Limits access to application files.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***
***Required Action:***
Type in the following command to check the ownership of the files in UNIX:

```
#ls -la $ORACLE_HOME
```

***Expected Results:***
Oracle account should be the owner of the directory.

***Comments:***
Only the oracle account has update permissions for the control files.

**Topic:** **Database Management System**
**SubTopic:** **File System Security**

***Objective 208***
Verify that a group has been defined for database users and that only authorized users are members of this group.

***Rationale:***
Limits database access to database users only.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
View the /etc/groups file to verify that a group has been created for oracle users.

***Expected Results:***
There should be an Oracle group defined in the file.

***Comments:***

**Topic:** **Database Management System**
**SubTopic:** **File System Security**

***Objective 209***
Verify that all database application files have the correct group permissions.

***Rationale:***
Restricts access to the application files.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Type the following command to check the permissions on the file in UNIX:

```
#ls -la $ORACLE_HOME
```

***Expected Results:***
The Oracle home directory should have only read/execute permissions for group.

***Comments:***
Only the oracle account should have update permissions to the control files.

**Topic:** **Database Management System**
**SubTopic:** **I & A**

***Objective 210***
Verify that NULL passwords are not used for database level logins.

***Rationale:***
Having a password provides extra protection and user authentication.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Login in as "system" using the sqlplus utility. Check in the system table DBA_USERS for null entries in the "password" column. Use the following sql command:

```
sql>SELECT username, password FROM DBA_USERS
```

***Expected Results:***
There should be no null entries in the "password" column.

***Comments:***

**Topic: Database Management System**
**SubTopic: I & A**

***Objective 211***
Verify that database client password encryption is configured and enabled.

***Rationale:***
Having an encrypted password from the client provides extra protection over the network.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Login as "system". Check the system table DBA_DB_LINKS for database link details and the username and password associated with the link.

```
sql>SELECT * FROM DBA_DB_LINKS
```

***Expected Results:***
The userids and password should not be hard coded in database links.

***Comments:***
Provides extra protection on remote accesses.

**Topic:** **Database Management System**
**SubTopic:** **I & A**

***Objective 224***
Verify that a single remote login account to the database application is not used for multiple remote users.

***Rationale:***
It reduces individual accountability on the server. Audit actions can be traced only to the local server login.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Login as "system". Check in the system table DBA_DB_LINKS to see that there are no PUBLIC database links.

```
sql> SELECT * FROM DBA_DB_LINKS
```

***Expected Results:***
None of the rows should have the value PUBLIC in the username column.

***Comments:***
Audit actions can be traced only to the local server login. A PUBLIC database link allows all users from the remote server access to the local server.

**Topic:** **Database Management System**
**SubTopic:** **I & A**

***Objective 246***
Verify that OS I&A is not used for database I&A.

***Rationale:***
Operating system account I&A is not to be used for database I&A.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Login as system. Check in the system table DBA_USERS to see if there are user names with an OPS$ prefix.

```
sql>SELECT username FROM DBA_USERS
```

***Expected Results:***
The user names should be without the OPS$ prefix.

***Comments:***
Having a separate database login account provides added security.

**Topic:** **Database Management System**
**SubTopic:** **Access Control**

***Objective 212***
Verify that permissions on the database system tables have not been modified.

***Rationale:***
Restricts access to the database.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Login as "system". Check in the DBA_SYS_PRIVS table to verify that no users have been granted the SELECT ANY TABLE system privilege.

```
sql>SELECT * FROM DBA_SYS_PRIVS
```

***Expected Results:***
No users with the SELECT ANY TABLE privilege.

***Comments:***
Restricts access to system tables.

**Topic:** **Database Management System**
**SubTopic:** **Access Control**

***Objective 251***
Verify that access to the database privileged account is restricted.

***Rationale:***
Restricts access to the database.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Login as "system". Check the table DBA_TABLES to see the application tables are not owned by privileged accounts. In addition, appliation tables should not be created in the "system" tablespace.

```
sql>SELECT table_name, username, tablespace_name from DBA_TABLES
```

***Expected Results:***
No application tables should be owned by the username "system" and should not be created in the "system" tablespace.

***Comments:***
Application tables should not be created under the "system" account. Access to the "system" account should be restricted. Application tables should not be created in the "system" tablespace to keep application database separate from system data.

**Topic:** **Database Management System**
**SubTopic:** **Access Control**

***Objective 219***
Verify that default passwords have been changed on any installation application login accounts or the login accounts have been deleted or locked after installation.

***Rationale:***
Restricts access to the database.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Attempt to logins to any default installation login accounts using install time passwords.

***Expected Results:***
Login should fail.

***Comments:***
The default password is the same for all Oracle products. The user "sys" is automatically enrolled and granted the DBA role.

**Topic:** **Database Management System**
**SubTopic:** **Access Control**

***Objective 214***
Determine if separation of user roles (e.g., SSO or SA) is enforced, and if so, ensure that different individuals have been assigned to these roles.

***Rationale:***
Role separation is an enhanced-security feature designed to provide checks and balances to administrative responsibilities.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Login as "system". Check for existing roles and the database system privileges in the DBA_ROLES and DBA_SYS_PRIVS system tables.

***Expected Results:***

***Comments:***
Application Administrators may assume the system administrator role for databases that are used only by one application. Roles help in dividing the set of powerful system privileges among more than one user and it distributes the control.

Having separation of privileges by roles provides individual accountability. Application Administrators may assume the system administrator role for databases that are used only by one application. Roles help in dividing the set of powerful system privileges among more than one user and it distributes the control. For additional security, passwords may be assigned to roles.

**Topic:** **Database Management System**
**SubTopic:** **Access Control**

***Objective 215***
Verify that permissions for privileged roles have not been modified from the database application defaults.

***Rationale:***
Restricts access to the database.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***
***Required Action:***
Login as "system" and check in the DBA_SYS_PRIVS to ensure that system privileges are not being propagated:

```
sql> SELECT * FROM DBA_SYS_PRIVS
```

***Expected Results:***
The column WITH ADMIN OPTION should have negative values.

***Comments:***
Restrict system-wide actions to a limited number of users.

***Step: 2***
***Required Action:***
Login as "system" abd check the resource profile of a user:

```
sql>SELECT * FROM DBA_PROFILES
```

***Expected Results:***
The resource allocated to a user should not be too large.

***Comments:***
Prevents excessive consumption of global database system resources.

**Topic:** **Database Management System**
**SubTopic:** **Access Control**

***Objective 216***
Verify that no database users are given the "grant with grant option" permission to database objects. If necessary, verify any users that have this permission are valid privileged database users.

***Rationale:***
To restrict the transmittal of access to database objects.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***
***Required Action:***
Login as "system". The system table DBA_SYS_PRIVS and DBA_ROLE_PRIVS contain description of system privileges and roles granted to users and to roles.

```
sql>SELECT * FROM DBA_SYS_PRIVS

sql>SELECT * FROM DBA_ROLE_PRIVS
```

***Expected Results:***
The column ADMIN OPTION signifies that the privilege can be granted further to another user or role. It should have a negative value.

***Comments:***
Restricts propagation of access privileges and roles.

***Step: 2***
***Required Action:***
Check in the system tables DBA_TAB_PRIVS and DBA_COL_PRIVS list all grants on objects and columns in the database.

```
sql>SELECT * FROM DBA_TAB_PRIVS

sql>SELECT*FROM DBA_COL_PRIVS
```

***Expected Results:***
The column GRANTABLE is set to YES if the grant is administered with a WITH GRANT OPTION, otherwise it is NO.

***Comments:***
Restricts propagation of access privileges and roles.

**Topic:** **Database Management System**
**SubTopic:** **Access Control**

***Objective 217***
Verify that guest application login accounts do not exist. Also verify that access to database objects is not granted to PUBLIC users.

***Rationale:***
Prevents public access to the database objects.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Login in as "system" and check in the system tables DBA_SYS_PRIVS, DBA_ROLE_PRIVS, DBA_TAB_PRIVS, DBA_COL_PRIVS to see that none of the privileges have been granted to PUBLIC.

```
sql>SELECT * FROM DBA_SYS_PRIVS
sql>SELECT * FROM DBA_ROLE_PRIVS
sql>SELECT * FROM DBA_TAB_PRIVS
sql>SELECT * FROM DBA_COL_PRIVS
```

***Expected Results:***
Special privileges and roles have not been granted to user group PUBLIC.

***Comments:***
Granting a privilege to PUBLIC implies that all database users have that privilege.

**Topic:** **Database Management System**
**SubTopic:** **Access Control**

***Objective 221***
Verify that stored procedures and triggers do not inadvertently accelerate general user permissions.

***Rationale:***
Permission to execute a stored procedure or a trigger gives a user indirect access to underlying database

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***
***Required Action:***
The system table `DBA_DEPENDENCIES` contains information on references between procedures and triggers. It can be used to determine the indirect access a user may get by having access to the procedure or trigger.

***Expected Results:***

***Comments:***
The user inherits access privileges of the creator of the stored procedure or the trigger. Therefore, permission to execute a stored procedure or a trigger gives a user indirect access to underlying database objects.

**Topic:** **Database Management System**
**SubTopic:** **Audit**

***Objective 222***
Verify that application level audits are generated for the vendor recommended events.

***Rationale:***
Ensures traceability of user actions.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Check in the database's parameter file (e.g., INIT.ORA) to see that auditing has been enabled. The system table DBA_AUDIT_TRAIL contains all audit records in the system. Other system tables containing audit relevant information are AUDIT_ACTIONS, DBA_AUDIT_STATEMENT, DBA_AUDIT_SESSION, DBA_AUDIT_OBJECT, and DBA_AUDIT_EXISTS.

***Expected Results:***
Enable auditing with the initialization parameter AUDIT_TRAIL. Turn on privileged auditing, statement auditing, and object auditing.

***Comments:***
Privileged auditing tracks the use of powerful system privileges without regard to specifically named objects. Statement auditing audits specific SQL statements without regard to specifically named objects. Object auditing audits accesses to specific schema objects. Actions performed on a parent table or a child table are audited by referential constraint.

Audit the actions performed on tables with referential constraints. Audit options are specified using the AUDIT command.

**Topic:** **Database Management System**
**SubTopic:** **Recovery Management**

***Objective 247***
Verify that the database redo log is configured correctly and it is being used.

***Rationale:***
Ensures recovery from failures.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***

***Expected Results:***
The redo log is being used in the ARCHIVELOG mode.

***Comments:***
Maintains two or more copies of the redo log on different disks. The database can be completely recovered from both instance and disk failure. Also the database can be backed up while it is open and available for use.

**Topic:** **Database Management System**
**SubTopic:** **Recovery Management**

***Objective 248***
Verify that important database configuration files and logs are being mirrored.

***Rationale:***
Ensures recovery from failures.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***

***Expected Results:***

***Comments:***
The database control files are being mirrored. The control files are used to guide the progression of the recovery procedure. The control files keep information about the file structure of the database and the current log sequence being written by the LGWR.

**Topic:** **Database Management System**
**SubTopic:**

***Objective 226***
Verify that application provided utilities are configured appropriately and are run on a regular basis.

***Rationale:***
Restricts access to database and maintains security.

***DII COE SRS Requirement:***

***Test Actions:***
***Step: 1***

***Required Action:***
Attempt to access the SQL*DBA or the SVRMGR utilities from a non-privileged account.

***Expected Results:***

***Comments:***
The SQL*DBA utility is available to perform special privileged DBA actions with additional operating system privileges.